arXiv:0808.3281v2 [cs.IT] 27 Dec 2008

ON THE DIAGONALIZATION OF THE DISCRETE FOURIER TRANSFORM

SHAMGAR GUREVICH AND RONNY HADANI

Dedicated to William Kahan and Beresford Parlett on the occasion of their 75th birthday

ABSTRACT. The discrete Fourier transform (DFT) is an important operator which acts on the Hilbert space of complex valued functions on the ring $\mathbb{Z}/N\mathbb{Z}$. In the case where $N = p$ is an odd prime number, we exhibit a canonical basis Φ of eigenvectors for the DFT. The transition matrix Θ from the standard basis to Φ defines a novel transform which we call the *discrete oscillator transform* (DOT for short). Finally, we describe a fast algorithm for computing Θ in certain cases.

0. INTRODUCTION

The discrete Fourier transform (DFT) is probably one of the most important operators in modern science. It is omnipresent in various fields of discrete mathematics and engineering, including combinatorics, number theory, computer science and, last but probably not least, digital signal processing. Formally, the DFT is a family $\{F_N\}$ of unitary operators, where each F_N acts on the Hilbert space $\mathcal{H}_N = \mathbb{C}(\mathbb{Z}/N\mathbb{Z})$ by the formula

$$F_N[f](w) = \frac{1}{\sqrt{N}} \sum_{t \in \mathbb{Z}/N\mathbb{Z}} e^{\frac{2\pi i}{N} wt} f(t).$$

Although so widely used, the spectral properties of the DFT remains to some extent still mysterious. For example, the calculation of the multiplicities of its eigenvalues, which was first carried out by Gauss, is quite involved and requires a multiple of number theoretic manipulations [1].

A primary motivation for studying the eigenvectors of the DFT comes from digital signal processing. Here, a function is considered in two basic realizations: The time realization and the frequency realization. Each realization, yields information on different attributes of the function. The DFT operator acts as a dictionary between these two realizations

$$\textbf{Time} \overset{F_N}{\rightleftarrows} \textbf{Frequency.}$$

From this point of view, it is natural to look for a diagonalization basis, namely, a basis of eigenvectors (eigen modes) for F_N. In this regard, the main conceptual difficulty comes from the fact that the diagonalization problem is ill-defined, since, F_N is an operator of order 4, i.e., $F_N^4 = Id$, which means that it has at most four eigenvalues $\pm 1, \pm i$, therefore each appears with large multiplicity (assuming $N \gg 4$).

Date: Dec. 1, 2007.

1

An interesting approach to the resolution of this difficulty, motivated from results in continuous Fourier analysis, was developed by Grünbaum in [8]. In that approach, a tridiagonal operator S_N which commutes with F_N and admits a simple spectrum is introduced. This enable him to give a basis of eigenfunctions for the DFT. Specifically, S_N appears as a certain discrete analogue of the differential operator $D = \partial_t^2 - t^2$ which commutes with the continuous Fourier transform. Other approaches can be found in [5, 16].

0.1. **Main results of this paper.**

In this paper we describe a representation theoretic approach to the diagonalization problem of the DFT in the case when $N = p$ is an odd prime number. Our approach, puts to the forefront the Weil representation [18] of the finite symplectic group $Sp = SL_2(\mathbb{F}_p)$ as the fundamental object underlying harmonic analysis in the finite setting (see [6, 11, 12, 13, 14, 17] for other recent applications of this point of view).

Specifically, we exhibit a canonical basis Φ_p of eigenvectors for the DFT. We also describe the transition matrix Θ_p from the standard basis to Φ_p, which we call the *discrete oscillator transform* (DOT for short). In addition, in the case $p \equiv 1 \, (\mathrm{mod} \, 4)$, we describe a fast algorithm for computing Θ_p (FOT for short). More precisely, we explain how in this case one can reduce the DOT to a composition of transforms with existing fast algorithms.

It is our general feeling that the Weil representation yields a transparent explanation to many classical results in finite harmonic analysis. In particular, we describe an alternative method for calculating the multiplicities of the eigenvalues for the DFT, a method we believe is more suggestive then the classical calculations.

The rest of the introduction is devoted to a more detailed account of the main ideas and results of this paper.

0.2. **Symmetries of the DFT.**

Let us fix an odd prime number p and for the rest of the introduction suppress the subscript p from all notations.

Generally, when a (diagonalizable) linear operator A has eigenvalues admitting large multiplicities, it suggest that there exists a group $G = G_A \subset GL(\mathcal{H})$ of "hidden" symmetries consisting of operators which commute with A. Alas, usually the problem of computing the group G is formidable and, in fact, equivalent to the problem of diagonalizing A. If the operator A arises "naturally", there is a chance that the group G can be effectively described. In preferred situations, G is commutative and large enough so that all degeneracies are resolved and the spaces of common eigenvectors with respect to G are one-dimensional. The basis of common eigenvectors with respect to G establishes a distinguish choice of eigenvectors for A. Philosophically, we can say that it is more correct to consider from start the group G instead of the single operator A.

Interestingly, the DFT operator F admits a natural group of symmetries G_F, which, in addition, can be effectively described using the Weil representation. For the sake of the introduction, it is enough to know that the Weil representation in this setting is a unitary representation $\rho : Sp \to U(\mathcal{H})$ and the key observation is that F is proportional to a single operator $\rho(\mathrm{w})$. The group G_F is the image under ρ of the centralizer subgroup T_w of w in Sp.

0.3. **The algebraic torus associated with the DFT.**

The subgroup T_w can be computed explicitly and is of a very "nice" type, it consists of rational points of a maximal algebraic torus in Sp which concretely means that it is maximal

commutative subgroup in Sp, consisting of elements which are diagonalizable over some field extension. Restricting the Weil representation to the subgroup T_{w} yields a collection $G_F = \{\rho(g) : g \in T_{\mathrm{w}}\}$ of commuting operators, each acts unitarily on the Hilbert space $\mathcal{H}$ and commutes with F. This, in turn, yields a decomposition, stable under Fourier transform, into character spaces

$$(0.1) \qquad\qquad \mathcal{H} = \bigoplus \mathcal{H}_\chi,$$

where χ runs in the set of (complex valued) characters of T_{w}, namely, $\phi \in \mathcal{H}_\chi$ iff $\rho(g)\phi = \chi(g)\phi$ for every $g \in T_{\mathrm{w}}$. The main technical statement of this paper, Theorem 2.2, roughly says that $\dim \mathcal{H}_\chi = 1$ for every χ which appears in (0.1).

0.4. **The oscillator transform.** Choosing a unit representative $\phi_\chi \in \mathcal{H}_\chi$ for every χ, gives the canonical basis $\Phi = \{\phi_\chi\}$ of eigenvectors for F. The oscillator transform Θ sends a function $f \in \mathcal{H}$ to the coefficients in the unique expansion

$$f = \sum a_\chi \phi_\chi.$$

The fine behavior of F and Θ is governed by the (split type) structure of T_{w}, which changes depending on the value of the prime p modulo 4. This phenomena has several consequences. In particular, it gives a transparent explanation to the precise way the multiplicities of the eigenvalues of F depend on the prime p. Another, algorithmic, consequence is related to the existence of a fast algorithm for computing Θ.

0.5. **Remarks.**

0.5.1. *Field extension.* All the results in this paper were stated for the basic finite field $\mathbb{F}_p$, for the reason of making the terminology more accessible. In fact, all the results can be stated and proved in essentially the same way for any field extension $\mathbb{F}_q$, $q = p^n$. One just need to replace p by q in all appropriate places. The only non-trivial statement in this respect is Corollary 4.2.

0.5.2. *Properties of eigenvectors.* The character vectors ϕ_χ satisfy many interesting properties and are objects of study in their own right. A comprehensive treatment of this aspect of the theory appears in [12, 14].

0.6. **Structure of the paper.** The paper consists of two main parts except of the introduction:

- In Section 1, we describe the Weil representation. We begin by discussing the finite Heisenberg group and the Heisenberg representation. Then, we introduce the Weil representation of the finite symplectic group, first it is described in abstract terms and then more explicitly invoking the idea of invariant presentation of an operator. In Section 2, we discuss the theory of tori in the one-dimensional Weil representation, and in Section 3, we explain how to associate to a maximal torus $T \subset Sp$ a transform Θ_T that we call the discrete oscillator transform. In addition, we describe a fast algorithm for computing Θ_T in the case T is a split torus. Finally, in Section 4, we apply the theory to the specific torus associated with the DFT operator. We finish this section with a treatment of the multiplicity problem for the DFT, from the representation theoretic perspective.

- We have two Appendices. Appendix A, consisting of proofs of statements which appeared in Sections 1-4, and Appendix B, consisting of an explicit formula for the particular oscillator transform Θ_{T_w} associated with the DFT.

0.7. **Acknowledgements.** It is a pleasure to thank our teacher J. Bernstein for his interest and guidance. We acknowledge R. Howe for sharing with us some of his thoughts concerning the finite Weil representation. We are happy to thank A. Sahai and N. Sochen for all of our discussions on the applied aspects of this work.

We appreciate several discussions we had with A. Grünbaum, W. Kahan, B. Parlett and B. Porat on the DFT. We thank A. Weinstein, J. Wolf and M. Zworski for interesting conversations related to the Weil representation. Finally, we thank P. Diaconis, M. Gu, M. Haiman, B. Poonen and K. Ribet for the opportunities to present this work in the MSRI, number theory, RTG and scientific computing seminars at Berkeley during February 2008.

1. The Weil representation

1.1. **The Heisenberg group.** Let (V, ω) be a two-dimensional symplectic vector space over the finite field $\mathbb{F}_p$. The reader should think of V as $\mathbb{F}_p \times \mathbb{F}_p$ with the standard form $\omega\left((t, w), (t', w')\right) = tw' - wt'$. Considering V as an abelian group, it admits a non-trivial central extension called the *Heisenberg* group. Concretely, the group H can be presented as the set $H = V \times \mathbb{F}_p$ with the multiplication given by

$$(v, z) \cdot (v', z') = (v + v', z + z' + \tfrac{1}{2}\omega(v, v')).$$

The center of H is $Z = Z(H) = \{(0, z) : z \in \mathbb{F}_p\}$. The symplectic group $Sp = Sp(V, \omega)$, which in this case is isomorphic to $SL_2(\mathbb{F}_p)$, acts by automorphism of H through its action on the V-coordinate.

1.2. **The Heisenberg representation.** One of the most important attributes of the group H is that it admits a special family of irreducible representations. The precise statement goes as follows. Let $\psi : Z \to \mathbb{C}^\times$ be a non-trivial character of the center. For example in this paper we take $\psi(z) = e^{\frac{2\pi i}{p} z}$. It is not hard to show

Theorem 1.1 (Stone-von Neuman)**.** *There exists a unique (up to isomorphism) irreducible unitary representation* $(\pi, H, \mathcal{H})$ *with the center acting by* ψ*, i.e.,* $\pi_{|Z} = \psi \cdot Id_{\mathcal{H}}$*.*

The representation π which appears in the above theorem will be called the *Heisenberg representation.*

1.2.1. *Standard realization of the Heisenberg representation.* The Heisenberg representation $(\pi, H, \mathcal{H})$ can be realized as follows: $\mathcal{H}$ is the Hilbert space $\mathbb{C}(\mathbb{F}_p)$ of complex valued functions on the finite line, with the standard Hermitian product. The action π is given by

- $\pi(t, 0)[f](x) = f(x + t)$;
- $\pi(0, w)[f](x) = \psi(wx) f(x)$;
- $\pi(z)[f](x) = \psi(z) f(x)$,

for every $f \in \mathcal{H}$, $x, t, w \in \mathbb{F}_p$ and $z \in Z$.

We call this explicit realization the *standard realization.*

1.3. **The Weil representation.** A direct consequence of Theorem 1.1 is the existence of a projective representation $\widetilde{\rho} : Sp \to PGL(\mathcal{H})$. The construction of $\widetilde{\rho}$ out of the Heisenberg representation π is due to Weil [18] and it goes as follows. Considering the Heisenberg representation π and an element $g \in Sp$, one can define a new representation π^g acting on the same Hilbert space via $\pi^g(h) = \pi(g(h))$. Clearly, both π and π^g have the same central character ψ, hence, by Theorem 1.1, they are isomorphic. Since the space $\mathsf{Hom}_H(\pi, \pi^g)$ is one-dimensional, choosing for every $g \in Sp$ a non-zero representative $\widetilde{\rho}(g) \in \mathsf{Hom}_H(\pi, \pi^g)$ gives the required projective Weil representation. In more concrete terms, the projective representation $\widetilde{\rho}$ is characterized by the formula

$$(1.1) \qquad \widetilde{\rho}(g)\,\pi(h)\,\widetilde{\rho}\left(g^{-1}\right) = \pi\left(g\left(h\right)\right),$$

for every $g \in Sp$ and $h \in H$. A more delicate statement is that there exists a unique lifting of $\widetilde{\rho}$ into a linear representation.

Theorem 1.2. *The projective Weil representation uniquely[1] lifts to a linear representation*

$$\rho : SL_2(\mathbb{F}_p) \longrightarrow GL(\mathcal{H}),$$

that satisfies equation (1.1).

The existence of a linearization ρ follows from a known fact [2] that any[2] projective representation of $SL_2(\mathbb{F}_p)$ can be linearized to an honest representation. The uniqueness follows from the well known fact (we give an argument in Appendix A) that the group $SL_2(\mathbb{F}_p)$, $p \neq 3$, is perfect, i.e., it has no non-trivial characters.

1.3.1. *Invariant presentation of the Weil representation.* Let us denote by $\mathbb{C}(H, \psi)$ the space of (complex valued) functions on H which are ψ-equivariant with respect to the action of the center, namely, a function $f \in \mathbb{C}(H, \psi)$ satisfies $f(zh) = \psi(z) f(h)$ for every $z \in Z$, $h \in H$. Given an operator $A \in \mathsf{End}(\mathcal{H})$, it can be written in a unique way as $A = \pi(K_A)$, where $K_A \in \mathbb{C}\left(H, \psi^{-1}\right)$ and π denotes the extended action $\pi(K_A) = \sum\limits_{h \in H} K_A(h)\,\pi(h)$. The function K_A is called the *kernel of A* and it is given by the *matrix coefficient*

$$(1.2) \qquad K_A(h) = \tfrac{1}{\dim \mathcal{H}} Tr\left(A\pi\left(h^{-1}\right)\right).$$

In the context of the Heisenberg representation, formula (1.2) is usually referred to as the *Weyl transform* [19].

Using the Weyl transform we are able to give an explicit description of the Weil representation. The idea [9] is to write each operator $\rho(g)$, $g \in Sp$, in terms of its kernel function $K_g = K_{\rho(g)} \in \mathbb{C}\left(H, \psi^{-1}\right)$. The following formula is taken from [9]

$$(1.3) \qquad K_g(v, z) = \tfrac{1}{\dim \mathcal{H}} \sigma\left(-\det\left(\kappa\left(g\right) + I\right)\right) \cdot \psi\left(\tfrac{1}{4}\omega\left(\kappa\left(g\right)v, v\right) + z\right)$$

for every $g \in Sp$ such that $g - I$ is invertible, where σ denotes the unique quadratic character (Legendre character) of the multiplicative group $\mathbb{F}_p^\times$ and $\kappa(g) = \frac{g+I}{g-I}$ is the Cayley transform.

---

[1]Uniquely, except in the case the finite field is $\mathbb{F}_3$. For the canonical choice in the latter case see [9].

[2]A more direct proof of the linearity of the Weil representation exists in [9, 10].

Remark 1.3. *Sketch of the proof of (1.3) (see details in* [9]*). First, one can easily show that*

$$K_g(v, z) = \frac{1}{\dim \mathcal{H}} \mu_g \cdot \psi\left(\frac{1}{4}\omega\left(\kappa\left(g\right)v, v\right) + z\right),$$

for $g \in Sp$ *with* $g - I$ *invertible, and for some* $\mu_g \in \mathbb{C}$*. Second, for* ρ *to be a linear representation the kernel* $K_g : H \to \mathbb{C}$ *should satisfy the multiplicativity property*

$$(1.4) \qquad\qquad\qquad K_{g_1 \cdot g_2} = K_{g_1} * K_{g_2},$$

where the $*$ *operation denotes convolution with respect to the Heisenberg group action. Finally, a direct calculation reveals that* μ_g *must be equal to* $\sigma\left(-\det\left(\kappa\left(g\right) + I\right)\right)$ *for (1.4) to hold. Hence, we obtain (1.3).*

2. The theory of tori in the Weil representation

2.1. **Tori.** A maximal (algebraic) torus in Sp is a maximal commutative subgroup which becomes diagonalizable over some field extension. There exists two conjugacy classes of maximal (algebraic) tori in Sp. The first class consists of those tori which are diagonalizable already over $\mathbb{F}_p$ or equivalently those are the tori that are conjugated to the standard diagonal torus

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_p \right\}.$$

A torus in this class is called a *split* torus. The second class consists of those tori which become diagonalizable over a quadratic extension $\mathbb{F}_{p^2}$ or equivalently those are tori which are not conjugated to A. A torus in this class is called a *non-split* torus (sometimes it is called inert torus).

Example 2.1 (Example of a non-split torus)**.** *It might be suggestive to explain further the notion of non-split torus by exploring, first, the analogue notion in the more familiar setting of the field* $\mathbb{R}$*. Here, the standard example of a maximal non-split torus is the circle group* $SO(2) \subset SL_2(\mathbb{R})$*. Indeed, it is a maximal commutative subgroup which becomes diagonalizable when considered over the extension field* $\mathbb{C}$ *of complex numbers. The above analogy suggests a way to construct an example of a maximal non-split torus in the finite field setting as well.*

Let us identify the symplectic plane $V = \mathbb{F}_p \times \mathbb{F}_p$ *with the quadratic extension* $\mathbb{F}_{p^2}$*. Under this identification,* $\mathbb{F}_{p^2}$ *acts on* V *and for every* $g \in \mathbb{F}_{p^2}$ *we have* $\omega\left(gu, gv\right) = \det\left(g\right)\omega\left(u, v\right)$*, which implies that the group*

$$T_{ns} = \left\{ g \in \mathbb{F}_{p^2}^\times : \det\left(g\right) = 1 \right\}$$

naturally lies in Sp*. The group* T_{ns} *is an example of a non-split torus which the reader might think of as the "finite circle".*

2.2. **Decompositions with respect to a maximal torus.** Restricting the Weil representation to a maximal torus $T \subset Sp$ yields a decomposition

$$(2.1) \qquad\qquad\qquad \mathcal{H} = \bigoplus_\chi \mathcal{H}_\chi,$$

where χ runs in the set $T^\vee$ of complex valued characters of the torus T. More concretely, choosing a generator[3] $t \in T$, the decomposition (2.1) naturally corresponds to the eigenspaces of the linear operator $\rho\left(t\right)$. The decomposition (2.1) depends on the split type of T. Let σ_T denote the unique quadratic character of T.

---

[3]A maximal torus T in $SL_2\left(\mathbb{F}_p\right)$ is a cyclic group, thus there exists a generator.

Theorem 2.2. *If T is a split torus then*

$$\dim \mathcal{H}_\chi = \begin{cases} 1 & \chi \neq \sigma_T, \\ 2 & \chi = \sigma_T. \end{cases}$$

If T is a non-split torus then

$$\dim \mathcal{H}_\chi = \begin{cases} 1 & \chi \neq \sigma_T, \\ 0 & \chi = \sigma_T. \end{cases}$$

For a proof see Appendix A.

3. THE OSCILLATOR TRANSFORM ASSOCIATED WITH A MAXIMAL TORUS

Let us fix a maximal torus $T \subset Sp$. Every vector $f \in \mathcal{H}$ can be written uniquely as a direct sum $f = \sum f_\chi$ with $f_\chi \in \mathcal{H}_\chi$ and χ runs in $I = \mathsf{Spec}_T(\mathcal{H})$ - the spectral support of $\mathcal{H}$ with respect to T consisting of all characters $\chi \in T^\vee$ such that $\dim \mathcal{H}_\chi \neq 0$. Let us choose, in addition, a collection of unit vectors $\phi_\chi \in \mathcal{H}_\chi$, $\chi \in I$, and let $\phi = \sum \phi_\chi$. We define the transform $\Theta_T = \Theta_{T,\phi} : \mathcal{H} \to \mathbb{C}(I)$ by

(3.1) $$\Theta_T[f](\chi) = \langle f, \phi_\chi \rangle.$$

We will call the transform Θ_T the *discrete oscillator transform* (DOT for short) with respect to the torus T and the test vector ϕ.

Remark 3.1. *We note that in the case T is a non-split torus, Θ_T maps $\mathcal{H}$ isomorphically to $\mathbb{C}(I)$. In the case T is a split torus, Θ_T has a kernel consisting of $f \in \mathcal{H}$ such that $\langle f, \phi_{\sigma_T} \rangle = 0$.*

3.1. **The oscillator transform (integral form).** Let $\mathcal{M}_T : \mathbb{C}(T) \to \mathbb{C}(T^\vee)$ denote the Mellin transform

$$\mathcal{M}_T[f](\chi) = \frac{1}{\#T} \sum_{g \in T} \overline{\chi}(g) f(g),$$

for $f \in \mathbb{C}(T)$, where $\overline{\chi}$ denotes the complex conjugate of χ. Let us denote by $m_T : \mathcal{H} \to \mathbb{C}(T)$ the matrix coefficient $m_T[f](g) = \langle f, \rho(g^{-1})\phi \rangle$ for $f \in \mathcal{H}$.

Lemma 3.2. *We have*

$$\Theta_T = \mathcal{M}_T \circ m_T.$$

For a proof see Appendix A.

3.2. **Fast oscillator transforms.** In practice, it is desirable to have a "fast" algorithm for computing the oscillator transform (FOT for short). We work in the following setting. The vector f is considered in the standard realization $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ (see 1.2.1). In this context the oscillator transform gives the transition matrix between the basis of delta functions and the basis $\Phi_T = \{\phi_\chi\}$ of character vectors. We will show that when T is a split torus and for an appropriate choice of ϕ, the oscillator transform can be computed in $O(p \log(p))$ arithmetic operations. Principally, what we will show is that the computation reduces to an application of DFT followed by an application of the standard Mellin transform, both transforms admit a fast algorithm [4].

Assume T is a split torus. Since all split tori are conjugated to one another, there exists, in particular, an element $s \in Sp$ conjugating T with the standard diagonal torus A. In more details, we have a homomorphism of groups $Ad_s : T \to A$ sending

$g \in T$ to $Ad_s(g) = sgs^{-1} \in A$. Dually, we have a homomorphism $Ad_s^\vee : A^\vee \to T^\vee$ between the corresponding groups of characters.

The main idea is to relate the oscillator transform with respect to T with the oscillator transform with respect to A. The relation is specified in the following simple lemma.

Lemma 3.3. *We have*

$$(3.2) \qquad\qquad (Ad_s^\vee)^* \circ \Theta_{T,\phi} = \Theta_{A,\rho(s)\phi} \circ \rho(s).$$

For the proof see Appendix A.

Remark 3.4. *Roughly speaking, (3.2) means that (up to a "reparametrization" of $T^\vee$ by $A^\vee$ using $Ad_s^\vee$) the oscillator transform of a vector $f \in \mathcal{H}$ with respect to the torus T is the same as the oscillator transform of the vector $\rho(s) f$ with respect to the diagonal torus A.*

In order to finish the construction of the fast algorithm we need to recall some well-known facts about the Weil representation in the standard realization.

First, we recall that the group Sp admits a Bruhat decomposition $Sp = B \cup BwB$, where B denote the Borel subgroup of lower triangular matrices and w denotes the Weyl element

$$(3.3) \qquad\qquad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Furthermore, the Borel subgroup B can be written as a product $B = AU = UA$, where A is the standard diagonal torus and U is the unipotent subgroup

$$U = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\}.$$

Therefore, we can write the Bruhat decomposition also as $Sp = UA \cup UwUA$.

Second, we give an explicit description of the operators in the Weil representation, associated with different types of elements in Sp. The operators are specified up to a unitary scalar:

- The standard torus A acts by (normalized) scaling: An element $g = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, acts by
$$S_a[f](x) = \sigma(a) f(a^{-1}x).$$

- The group U of unipotent matrices acts by quadratic characters (chirps): An element $g = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$, acts by
$$M_b[f](x) = \psi(-\tfrac{b}{2}x^2) f(x).$$

- The Weyl element w acts by discrete Fourier transform
$$F[f](y) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \psi(yx) f(x).$$

The above formulas can be easily verified using identity (1.1). Hence, we conclude that every operator $\rho(g)$, $g \in Sp$, can be written either in the form $\rho(g) = M_b \circ S_a$

or in the form $\rho\left(g\right) = M_{b_2} \circ F \circ M_{b_1} \circ S_a$. In particular, given a function $f \in \mathbb{C}\left(\mathbb{F}_p\right)$, applying formula (3.2) with $\phi = \rho\left(s\right)^{-1}\delta_1$ yields

$$(3.4) \qquad \Theta_{T,\phi}\left[f\right]\left(Ad_s^\vee\left(\chi\right)\right) = \frac{1}{p-1}\sum_{a \in \mathbb{F}_p^\times}\sigma\left(a\right)\overline{\chi}\left(a\right)\rho\left(s\right)\left[f\right]\left(a\right),$$

for every $\chi \in A^\vee$, where s is the specific element that conjugate T to A.

In conclusion, formula (3.4) implies that $\Theta_{T,\phi}\left[f\right]$ can be computed by, first, applying the (DFT type) operator $\rho\left(s\right)$ to f and then applying Mellin transform to the result. This completes our construction of the Fast Oscillator Transform in the split case.

Problem 3.5. *Does there exists a fast algorithm for computing the oscillator transform associated to a **non-split** torus?*

4. DIAGONALIZATION OF THE DISCRETE FOURIER TRANSFORM

In this section we apply the previous development in order to exhibit a canonical basis of eigenvectors for the DFT.

4.1. Relation between the DFT and the Weil representation.

We will show that the DFT can be naturally identified (up to a normalization scalar) with an operator $\rho\left(\mathrm{w}\right)$ in the Weil representation, where w is an element in a maximal torus $T_{\mathrm{w}} \subset Sp$. We take $\mathrm{w} \in Sp$ to be the Weyl element (3.3).

Theorem 4.1. *We have*

$$F = C \cdot \rho\left(\mathrm{w}\right),$$

where $C = i^{\frac{p-1}{2}}$.

Corollary 4.2. *In case one considers a field extension of the form $\mathbb{F}_q$, $q = p^d$ and the additive character $\psi_q : \mathbb{F}_q \to \mathbb{C}^\times$, given by $\psi_q(x) = \psi\left(tr\left(x\right)\right)$. In this case, the Fourier transform F associated with ψ_q and the operator $\rho\left(\mathrm{w}\right)$ coming from the Weil representation of $SL_2(\mathbb{F}_q)$, are related by*

$$F = C \cdot \rho\left(\mathrm{w}\right),$$

with $C = (-1)^{d-1}i^{d\frac{p-1}{2}}$.

For the proofs see Appendix A.

4.2. Diagonalization of the DFT.

Theorem 4.1 implies that the diagonalization problems of the operators F and $\rho\left(\mathrm{w}\right)$ are equivalent. The second problem can be approached using representation theory, which is what we are going to do next.

Let us denote by T_{w} the centralizer of w in Sp, namely T_{w} consists of all elements $g \in Sp$ such that $g\mathrm{w} = \mathrm{w}g$, in particular we have that $\mathrm{w} \in T_{\mathrm{w}}$.

Proposition 4.3. *The group T_{w} is a maximal torus. Moreover the split type of T_{w} depends on the prime p in the following way: T_{w} is a split torus when $p \equiv 1\,(\mathrm{mod}\,4)$ and is a non-split torus when $p \equiv 3\,(\mathrm{mod}\,4)$.*

For a proof see Appendix A.

Proposition 4.3 has several consequences. First consequence is that choosing a unit character vector $\phi_\chi \in \mathcal{H}_\chi$ for every $\chi \in \mathsf{Spec}_{T_{\mathrm{w}}}\left(\mathcal{H}\right)$ gives a canonical (up to

normalizing unitary constants) choice of eigenvectors for the DFT [4]. Second, more mysterious consequence is that although the formula of the DFT is uniform in p, its qualitative behavior changes dramatically between the cases when $p \equiv 1 \,(\mathrm{mod}\,4)$ and $p \equiv 3 \,(\mathrm{mod}\,4)$. This is manifested in the structure of the group of symmetries: In the first case, the group of symmetries is a split torus consisting of $p-1$ elements and in the second case it is a non-split torus consisting of $p + 1$ elements. It also seems that the structure of the symmetry group is important from the algorithmic perspective, in the case $p \equiv 1 \,(\mathrm{mod}\,4)$ we built a fast algorithm for computing $\Theta = \Theta_{T_{\mathrm{w}}}$, while in the case $p \equiv 3 \,(\mathrm{mod}\,4)$ the existence of such an algorithm remains open (see Problem 3.5).

For the convenience of the reader, we enclose in Appendix B an explicit formula for $\Theta_{T_{\mathrm{w}}}$ in the case $p \equiv 1 \,(\mathrm{mod}\,4)$.

4.3. **Multiplicities of eigenvalues of the DFT.** Considering the group T_{w} we can give a transparent computation of the eigenvalues multiplicities for the operator $\rho(\mathrm{w})$. First we note that, since w is an element of order 4, the eigenvalues of $\rho(\mathrm{w})$ lies in the set $\{\pm 1, \pm i\}$. For $\lambda \in \{\pm 1, \pm i\}$, let m_λ denote the multiplicity of the eigenvalue λ. We observe that

$$m_\lambda = \bigoplus_{\chi \in I_\lambda} \dim \mathcal{H}_\chi,$$

where I_λ consists of all characters $\chi \in \mathsf{Spec}_{T_{\mathrm{w}}}(\mathcal{H})$ such that $\chi(\mathrm{w}) = \lambda$. The result now follows easily from Theorem 2.2, applied to the torus T_{w}. We treat separately the split and non-split cases.

- Assume T_{w} is a split torus, which happens when $p = 1 \,(\mathrm{mod}\,4)$, namely, $p = 4l + 1$, $l \in \mathbb{N}$. Since $\dim \mathcal{H}_\chi = 1$ for $\chi \neq \sigma_{T_{\mathrm{w}}}$ it follows that $m_{\pm i} = \frac{p-1}{4} = l$. We are left to determine the values of $m_{\pm 1}$, which depend on whether $\sigma_{T_{\mathrm{w}}}(\mathrm{w}) = \mathrm{w}^{\frac{p-1}{2}}$ is 1 or -1. Since w is an element of order 4 in T_{w} we get that

$$\sigma_{T_{\mathrm{w}}}(\mathrm{w}) = \begin{cases} 1, & p \equiv 1 \,(\mathrm{mod}\,8), \\ -1, & p \equiv 5 \,(\mathrm{mod}\,8), \end{cases}$$

  which implies that when $p \equiv 1 \,(\mathrm{mod}\,8)$ then $m_1 = l + 1$ and $m_{-1} = l$ and when $p \equiv 5 \,(\mathrm{mod}\,8)$ then $m_1 = l$ and $m_{-1} = l + 1$.

- Assume T_{w} is a non-split torus, which happens when $p \equiv 3 \,(\mathrm{mod}\,4)$, namely, $p = 4l + 3$, $l \in \mathbb{N}$. Since $\dim \mathcal{H}_\chi = 1$ for $\chi \neq \sigma_{T_{\mathrm{w}}}$ it follows that $m_{\pm i} = \frac{p+1}{4} = l + 1$. The values of $m_{\pm 1}$ depend on whether $\sigma_{T_{\mathrm{w}}}(\mathrm{w}) = \mathrm{w}^{\frac{p+1}{2}}$ is 1 or -1. Since w is an element of order 4 in T_{w} we get that

$$\sigma_{T_{\mathrm{w}}}(\mathrm{w}) = \begin{cases} 1, & p \equiv 7 \,(\mathrm{mod}\,8), \\ -1, & p \equiv 3 \,(\mathrm{mod}\,8), \end{cases}$$

  which implies that when $p \equiv 7 \,(\mathrm{mod}\,8)$ then $m_1 = l$ and $m_{-1} = l + 1$ and when $p \equiv 3 \,(\mathrm{mod}\,8)$ then $m_1 = l + 1$ and $m_{-1} = l$.

---

[4]In the case T_w is a split torus there is a slight ambiguity in the choice of a character vector with respect to σ_{T_w}. This ambiguity can be resolved by further investigation which we will not discuss here.

Summarizing, the multiplicities of the operator $\rho\,(\mathrm{w})$ are

(4.1)

	m_1	m_{-1}	m_i	m_{-i}
$p = 8k + 1$	$2k + 1$	$2k$	$2k$	$2k$
$p = 8k + 3$	$2k$	$2k + 1$	$2k + 1$	$2k + 1$
$p = 8k + 5$	$2k + 1$	$2k + 2$	$2k + 1$	$2k + 1$
$p = 8k + 7$	$2k + 2$	$2k + 1$	$2k + 2$	$2k + 2$

Considering now the DFT operator F. If we denote by n_μ, $\mu \in \{\pm 1, \pm i\}$ the multiplicity of the eigenvalue μ of F then the values of n_μ can be deduced from table (4.1) by invoking the relation $n_\mu = m_\lambda$ where $\lambda = i^{\frac{p-1}{2}} \cdot \mu$ (see Theorem 4.1). Summarizing, the multiplicities of the DFT are

	n_1	n_{-1}	n_i	n_{-i}
$p = 4l + 1$	$l + 1$	l	l	l
$p = 4l + 3$	$l + 1$	$l + 1$	$l + 1$	l

For a comprehensive treatment of the multiplicity problem from a more classical point of view see [1]. Other applications of Theorem 4.1 appear in [11].

APPENDIX A. PROOFS

A.1. **Proof of Theorem 1.2.** We are left to proof the uniqueness in the case $p \neq 3$. Since any two linearizations differ by a character of $SL_2(\mathbb{F}_p)$, the uniqueness follows from the fact that $SL_2(\mathbb{F}_p)$ is a perfect group, namely, it admits no non-trivial characters.

For the sake of completeness let us prove the last assertion

Proposition A.1. *The group $SL_2(\mathbb{F}_p)$ is perfect.*

Indeed, let us consider a character $\chi : SL_2(\mathbb{F}_p) \to \mathbb{C}^\times$. On the one hand, considering the pull-back character $\chi \circ pr$, where $pr : SL_2(\mathbb{Z}) \to SL_2(\mathbb{F}_p)$ is the canonical projection, one obtains that $(\chi \circ pr)^{12} = 1$ since the group of characters of $SL_2(\mathbb{Z})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ [3]. Now, since pr is a surjection, this implies that $\chi^{12} = 1$.

On the other hand, the group $SL_2(\mathbb{F}_p)$ is generated by the unipotent elements

$$u_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad u_- = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

and since $u_+^p = u_-^p = 1$, we have $\chi^n = 1$. Hence, $\chi = 1$ because $\gcd(12, p) = 1$. This concludes the proof of the theorem.

A.2. **Proof of Theorem 2.2.** Fix a character $\chi : T \to \mathbb{C}^\times$. Let P_χ denote the orthogonal projector on the subspace $\mathcal{H}_\chi$. We have $\dim \mathcal{H}_\chi = Tr\,(P_\chi)$. The projector P_χ can be written in terms of the Weil representation, namely

$$P_\chi = \frac{1}{\#T} \sum_{g \in T} \overline{\chi}\,(g)\,\rho\,(g).$$

Therefore

$$
\begin{aligned}
Tr\left(P_{\chi}\right) &= \frac{1}{\#T}\sum_{g\in T}\overline{\chi}\left(g\right)Tr\left(\rho\left(g\right)\right)\\
&= \frac{\dim\mathcal{H}}{\#T}\sum_{g\in T}\overline{\chi}\left(g\right)K_{g}\left(0\right),
\end{aligned}
$$

where in the second equality we use the definition of the kernel function K_{g}. Invoking formula (1.3) we obtain

$$
(A.1)\qquad Tr\left(P_{\chi}\right)=\frac{1}{\#T}\left(\sigma\left(-1\right)\left(\sum_{g\in T^{\times}}\overline{\chi}\left(g\right)\sigma\left(\det\left(\kappa\left(g\right)+I\right)\right)\right)+\dim\mathcal{H}\right),
$$

where $T^{\times}=T-\{1\}$.

Lemma A.2. *For every $g\in T^{\times}$, $\sigma\left(\det\left(\kappa\left(g\right)+I\right)\right)=\sigma_{T}\left(-1\right)\sigma_{T}\left(g\right)$.*

Using the above lemma and substituting $\dim\mathcal{H}=p$ in (A.1) we obtain the following basic formula

$$
(A.2)\qquad Tr\left(P_{\chi}\right)=\frac{1}{\#T}\left(\sigma\left(-1\right)\sigma_{T}\left(-1\right)\left(\sum_{g\in T^{\times}}\overline{\chi}\left(g\right)\sigma_{T}\left(g\right)\right)+p\right).
$$

Next, we analyze (A.2) separately according to the split type of T. In our computations we use the simple yet important fact that the quadratic character σ_{T} can be written explicitly as $\sigma_{T}\left(g\right)=g^{\frac{\#T}{2}}\in\{1,-1\}$.

- T split. In this case $\#T=p-1$, thus $\sigma_{T}\left(g\right)=g^{\frac{p-1}{2}}$, which implies that $\sigma\left(-1\right)\sigma_{T}\left(-1\right)=1$. Consequently

$$
\begin{aligned}
Tr\left(P_{\chi}\right) &= \frac{1}{p-1}\left(\left(\sum_{g\in T^{\times}}\overline{\chi}\left(g\right)\sigma_{T}\left(g\right)\right)+p\right)\\
&= \begin{cases} \frac{1}{p-1}\left(-1+p\right) & \chi\neq\sigma_{T},\\ \frac{1}{p-1}\left(2p-2\right) & \chi=\sigma_{T}, \end{cases}\\
&= \begin{cases} 1 & \chi\neq\sigma_{T},\\ 2 & \chi=\sigma_{T}. \end{cases}
\end{aligned}
$$

- T non-split. In this case $\#T=p+1$, thus $\sigma_{T}\left(g\right)=g^{\frac{p+1}{2}}$, which implies that $\sigma\left(-1\right)\sigma_{T}\left(-1\right)=\left(-1\right)^{\frac{p-1}{2}+\frac{p+1}{2}}=-1$. Consequently

$$
\begin{aligned}
Tr\left(P_{\chi}\right) &= \frac{1}{p+1}\left(-\left(\sum_{g\in T^{\times}}\overline{\chi}\left(g\right)\sigma_{T}\left(g\right)\right)+p\right)\\
&= \begin{cases} \frac{1}{p+1}\left(1+p\right) & \chi\neq\sigma_{T},\\ \frac{1}{p+1}\left(-p+p\right) & \chi=\sigma_{T}, \end{cases}\\
&= \begin{cases} 1 & \chi\neq\sigma_{T},\\ 0 & \chi=\sigma_{T}. \end{cases}
\end{aligned}
$$

This concludes the proof of the theorem.

A.2.1. *Proof of Lemma A.2.* Let $U \subset Sp$ be the subset consisting all elements $g \in Sp$ such that $g - I$ is invertible. Define $\varepsilon : U \to \mathbb{C}$, as $\varepsilon(g) = \sigma(\det(\kappa(g) + 1))$. We note that U is closed under conjugation and ε is conjugation invariant. We treat the split and non-split cases separately.

Assume T split. Since ε is conjugation invariant, it is enough to show that $\varepsilon(g) = \sigma_T(-1)\sigma_T(g)$ when T is the standard diagonal torus A. Let $g = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ $\in A$. We have

$$
\begin{aligned}
\det(\kappa(g) + 1) &= \left(1 + \frac{a+1}{a-1}\right)\left(1 - \frac{a+1}{a-1}\right) \\
&= \frac{-4a}{(a-1)^2},
\end{aligned}
$$

therefore $\varepsilon(g) = \sigma(-1)\sigma(a) = \sigma_T(-1)\sigma_T(g)$. Concluding the argument in this case.

Assume T is non-split. Again by conjugation invariance, we can assume that T consists of elements $g \in \mathbb{F}_{p^2}^\times$ such that $\det(g) = g^{p+1} = 1$. We have

$$
\kappa(g) + 1 = \frac{g+1}{g-1} + 1 = \frac{2g}{g-1},
$$

hence

$$
\det(\kappa(g) + 1) = \left(\frac{2g}{g-1}\right)^{p+1} = \frac{4}{(g-1)^{p+1}},
$$

and

$$
\varepsilon(g) = \sigma\left(\frac{4}{(g-1)^{p+1}}\right) = \left(\frac{1}{(g-1)^{p+1}}\right)^{\frac{p-1}{2}} = \left(\frac{1}{(g-1)^{p-1}}\right)^{\frac{p+1}{2}}.
$$

Explicit computation reveals that $\frac{1}{(g-1)^{p-1}} = -g$, therefore we obtain

$$
\varepsilon(g) = (-g)^{\frac{p+1}{2}} = \sigma_T(-1)\sigma_T(g).
$$

Concluding the argument in this case and the proof of the lemma.

A.3. **Proof of Lemma 3.2.** The proof is by direct verification. Write

$$
\begin{aligned}
\mathcal{M}_T \circ m_T[\chi] &= \frac{1}{\#T}\sum_{g \in T}\overline{\chi}(g)\left\langle f, \rho(g)^{-1}\phi\right\rangle \\
&= \left\langle f, \frac{1}{\#T}\sum_{g \in T}\chi(g)\rho(g^{-1})\phi\right\rangle \\
&= \left\langle f, \left(\frac{1}{\#T}\sum_{g \in T}\overline{\chi}(g)\rho(g)\right)\phi\right\rangle \\
&= \langle f, P_\chi\phi\rangle = \langle f, \phi_\chi\rangle = \Theta_{T,\phi}[f](\chi).
\end{aligned}
$$

A.4. **Proof of Lemma 3.3.** The proof is by direct computation. Let $f \in \mathcal{H}$ and $\chi \in A^{\vee}$.

$$
\begin{aligned}
\left(Ad_s^{\vee}\right)^* \circ \Theta_{T,\phi}\left[f\right]\left(\chi\right) &= \Theta_{T,\phi}\left[f\right]\left(Ad_s^{\vee}\left(\chi\right)\right) \\
&= M_T \circ m_{T,\phi}\left[f\right]\left(Ad_s^{\vee}\left(\chi\right)\right) \\
&= \frac{1}{\#T}\sum_{g \in T}\overline{Ad_s^{\vee}\left(\chi\right)}\left(g\right)\left\langle f, \rho\left(g^{-1}\right)\phi\right\rangle \\
&= \frac{1}{\#T}\sum_{g \in T}\overline{\chi}\left(sgs^{-1}\right)\left\langle f, \rho\left(g^{-1}\right)\phi\right\rangle \\
&= \frac{1}{\#T}\sum_{g \in A}\overline{\chi}\left(g\right)\left\langle f, \rho\left(\left(s^{-1}gs\right)^{-1}\right)\phi\right\rangle \\
&= \frac{1}{\#T}\sum_{g \in A}\overline{\chi}\left(g\right)\left\langle \rho\left(s\right)f, \rho\left(g^{-1}\right)\rho\left(s\right)\phi\right\rangle \\
&= \frac{1}{\#A}\sum_{g \in A}\overline{\chi}\left(g\right)\left\langle \rho\left(s\right)f, \rho\left(g^{-1}\right)\rho\left(s\right)\phi\right\rangle \\
&= M_A \circ m_{A,\rho(s)\phi}\left[\rho\left(s\right)f\right]\left(\chi\right) = \Theta_{A,\rho(s)\phi}\left[\rho\left(s\right)f\right]\left(\chi\right).
\end{aligned}
$$

This concludes the proof of the lemma.

A.5. **Proof of Theorem 4.1.** The operator $\rho\left(\mathrm{w}\right)$ is characterized up to a unitary scalar by the identity (see formula (1.1)) $\rho\left(\mathrm{w}\right)\pi\left(h\right)\rho\left(\mathrm{w}\right)^{-1} = \pi\left(\mathrm{w}\left(h\right)\right)$ for every $h \in H$. Explicit computation reveals that for every $h \in H$, $F \circ \pi\left(h\right) \circ F^{-1} = \pi\left(\mathrm{w}\left(h\right)\right)$, which implies that $F = C \cdot \rho\left(\mathrm{w}\right)$.

Next, computing the determinant of both sides we get $\det\left(F\right) = C^p \cdot \det\left(\rho\left(\mathrm{w}\right)\right)$.

Claim A.3. *We have* $\det\left(\rho\left(\mathrm{w}\right)\right) = 1$.

Since $\det(\rho(\mathrm{w})) = 1$, we have

(A.3) $$\det\left(F\right) = C^p.$$

In addition

Proposition A.4. *We have*

(A.4) $$\det\left(F\right) = i^{\frac{p(p-1)}{2}}.$$

From the relations $F^4 = \rho\left(\mathrm{w}\right)^4 = Id_{\mathcal{H}}$ we get that $C^4 = 1$. Since $\gcd\left(4,p\right) = 1$ we conclude from (A.3) and (A.4) that $C = i^{\frac{p-1}{2}}$.

A.5.1. *Proof of Claim A.3.* In fact, in case $p \neq 3$, ρ is unimodular, i.e., $\det\left(\rho\left(g\right)\right) = 1$ for every $g \in SL_2(\mathbb{F}_p)$. Indeed, the perfectness of $SL_2(\mathbb{F}_p)$ (see Proposition A.1) implies that $\det\left(\rho\left(g\right)\right) = 1$, for every $g \in SL_2(\mathbb{F}_p)$, since $\det \circ \rho$ is a character of $SL_2(\mathbb{F}_p)$. In order to cover also the case of the field $\mathbb{F}_3$, we give an alternative argument as follow. Since $\det \circ \rho$ is a character of $SL_2(\mathbb{F}_p)$, we have $(\det \circ \rho(\mathrm{w}))^p = 1$ (see the argument in A.1). However, the element w is of order 4, which implies $\det\left(\rho\left(\mathrm{w}\right)\right)^4 = 1$. The claim now follows since $\gcd(4,p) = 1$.

A.5.2. *Proof of Proposition A.4.* Consider the matrix of $\sqrt{p}F$. If we write ψ in the form $\psi(x) = \zeta^x$, $x = 0,.., p-1$ and $\zeta = e^{\frac{2\pi i}{p}}$, then the matrix of F takes the form $(\zeta^{yx} : x,y \in \{0,1,..,p-1\})$, hence it is a *Vandermonde matrix*. Applying the formula ([7]) for the determinant of the Vandermonde matrix, we get

$$
\begin{aligned}
\text{(A.5)} \quad \det(\sqrt{p}F) &= \prod_{0 \le x < y \le p-1} (\zeta^y - \zeta^x) = \prod_{0 \le x < y \le p-1} (\psi(y) - \psi(x)) \\
&= \prod_{0 \le x < y \le p-1} \psi(\tfrac{x+y}{2}) \prod_{0 \le x < y \le p-1} \left(\psi(\tfrac{y-x}{2}) - \psi(\tfrac{x-y}{2}) \right) \\
&= \psi(0) \cdot i^{\frac{p(p-1)}{2}} \cdot 2^{\frac{p(p-1)}{2}} \prod_{j=1}^{p-1} (\sin(\tfrac{\pi \cdot j}{p}))^{p-j},
\end{aligned}
$$

where the equality $\prod_{0 \le x < y \le p-1} \psi(\frac{x+y}{2}) = \psi(0)$ follows from the fact that $\sum_{0 \le x < y \le p-1} (x+y) = \frac{1}{2}\{ \sum_{x,y \in \mathbb{F}_p} (x+y) - \sum_{x=y \in \mathbb{F}_p} (x+y)\} = 0 - 0 = 0$.

Taking the absolute value on both sides of (A.5), gives us

$$
p^{\frac{p}{2}} = 2^{\frac{p(p-1)}{2}} \prod_{j=1}^{p-1} (\sin(\tfrac{\pi \cdot j}{p}))^{p-j},
$$

hence $\det(F) = i^{\frac{p(p-1)}{2}}$ as claimed.

A.6. **Proof of Corollary 4.2.** Taking the trace on both sides of the equation $F = C \cdot \rho(\mathrm{w})$, using the explicit formula for the character of the Weil representation obtained from formula (1.3), and noting that $\sqrt{q}Tr(F) = \sum_{x \in \mathbb{F}_q} \psi_q(x^2)$, the claim follows from the Hasse–Davenport relation [15]

$$
- \sum_{x \in \mathbb{F}_q} \psi_q(x^2) = (- \sum_{x \in \mathbb{F}_p} \psi(x^2))^d.
$$

A.7. **Proof of proposition 4.3.** In order to show that T_w are the rational points of an algebraic torus, it is enough to show that the characteristic polynomial of $\mathrm{w} \in SL_2(\mathbb{F}_p)$ has distinct eigenvalues. We have $\chi_\mathrm{w}(t) = \det(tI - \mathrm{w}) = t^2 + 1$ which has roots $\pm\sqrt{-1}$. Looking at $\chi_\mathrm{w}(t)$ we see that T_w is a split torus when -1 admits a square root in $\mathbb{F}_p$, that is when $\sigma(-1) = (-1)^{\frac{p-1}{2}} = 1$ which happens when $p \equiv 1 \pmod 4$. Concluding the proof of the proposition.

APPENDIX B. EXPLICIT FORMULAS FOR THE OSCILLATOR TRANSFORM

Looking at formula (3.4) of the oscillator transform Θ_{T_w}, in the case $p \equiv 1$ (mod 4), we see that in order to have an explicit description we need to describe the operator $\rho(s)$, where $s \in Sp$ is an element which conjugates the torus T_w to the standard torus A.

It is enough to describe $\rho(s)$ up to a unitary scalar, which is what we are going to do. Since, we assume that $p \equiv 1 \pmod 4$, there exist an element $\epsilon \in \mathbb{F}_p^\times$, which satisfies $\epsilon^2 = -1$. Let

$$
s = \begin{pmatrix} \frac{1}{2} & \frac{\epsilon}{2} \\ \epsilon & 1 \end{pmatrix}.
$$

Direct verification reveals that $sT_{\mathrm{w}}s^{-1} = A$. Now, the element s can be decomposed according to the Bruhat decomposition

$$s = \begin{pmatrix} \frac{1}{2} & \frac{\epsilon}{2} \\ \epsilon & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{2}{\epsilon} & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{\epsilon}{4} & 1 \end{pmatrix} \begin{pmatrix} \frac{2}{\epsilon} & 0 \\ 0 & \frac{\epsilon}{2} \end{pmatrix},$$

which implies, using the explicit formulas which appears in Section 3.2, that

$$\rho(s) = C \cdot M_{\frac{2}{\epsilon}} \circ F \circ M_{\frac{\epsilon}{4}} \circ S_{\frac{2}{\epsilon}},$$

where C is some unitary scalar.

References

[1] Auslander L. and Tolimieri R., Is computing with the finite Fourier transform pure or applied mathematics? *Bull. Amer. Math. Soc. (N.S.)* **1** (1979), no. 6, 847-897.

[2] Beyl F.R., The Schur multiplicator of $SL(2, \mathbb{Z}/m\mathbb{Z})$ and the congruence subgroup property *Math. Zeit. 191* (1986).

[3] Coxeter H.S.M. and Moser, W.O.J., Generators and relations for discrete groups. *Ergebnisse der Mathematik und ihrer Grenzgebiete, 14. Springer-Verlag, Berlin-New York* (1980).

[4] Cooley J.W. and Tukey J.W., An algorithm for the machine calculation of complex Fourier series. Math. Comput. 19, 297–301 (1965).

[5] Dickinson B.W. and Steiglitz K., Eigenvectors and functions of the discrete Fourier transform. *IEEE Tans. Acoustics Speech Signal Proc. 30 no. 1, 25-31* (1982).

[6] Feichtinger H.G., Hazewinkel M., Kaiblinger N., Matusiak E. and Neuhauser M., Metaplectic operators on $\mathbb{C}^n$. *Q.J. Math. 59 no. 1, 15-28,* (2008).

[7] Fulton W. and Harris J., Representation theory. A first course. *Graduate Texts in Mathematics, 129. Readings in Mathematics. Springer-Verlag, New York* (1991).

[8] Grünbaum F. A., The eigenvectors of the discrete Fourier transform. *J. Math. Anal. Appl. 88, 355-363.* (1982).

[9] Gurevich S. and Hadani R., The geometric Weil representation. *Selecta Mathematica, New Series, Birkhäuser Basel* (Accepted: Dec. 2006).

[10] Gurevich S. and Hadani R., Quantization of symplectic vector spaces over finite fields. *arXiv:0705.4556* (2005).

[11] Gurevich S., Hadani R. and Howe R., Quadratic reciprocity and sign of Gauss sum via the finite Weil representation. *Submitted* (2008).

[12] Gurevich S., Hadani R. and Sochen N., The finite harmonic oscillator and its associated sequences. *Proceedings of the National Academy of Sciences of the United States of America (PNAS), July 22, 2008, vol. 105 no. 29 9869-9873* (2008).

[13] Gurevich S., Hadani R. and Sochen N., On some deterministic dictionaries supporting sparsity. *To appear in the special issue on sparsity (Editors: A. Cohen, R. DeVore, M. Elad, A. Gilbert) of the Journal of Fourier Analysis and its Applications* (2008).

[14] Gurevich S., Hadani R. and Sochen N., The finite harmonic oscillator and its application to sequences, communication and radar. *To appear in the IEEE Transaction on Information Theory* (2008).

[15] Hasse H. and Davenport H., Die Nullstelen der Kongruenzzetafunktionen in gewissen zyklischen Fallen, *J. Reine Angew. Math. 172* (1934), 151-182.

[16] Mehta M.L., Eigenvalues and Eigenvectors of the finite Fourier transform. *J. Math. Phys. 28, no. 4, 781-785 (1987).*

[17] Vourdas A. Quantum systems with finite Hilbert space: Galois fields in quantum mechanics. *J.Phys. A 40, no. 33, R285-R331 (2007).*

[18] Weil A., Sur certains groupes d'operateurs unitaires. *Acta Math. 111* (1964) 143-211.

[19] Weyl H., Gruppentheorie und Quantenmechanik. *1st edition Hirzel, Leipzig* (1928).

Department of Mathematics, University of California, Berkeley, CA 94720, USA.
E-mail address: shamgar@math.berkeley.edu

Department of Mathematics, University of Chicago, IL, 60637, USA.
E-mail address: hadani@math.uchicago.edu